UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/925,031 | 08/08/2001 | Giovanni Di Bernardo | 854063.646 | 2519 |

500 7590 01/19/2006

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVE
SUITE 6300
SEATTLE, WA 98104-7092

| EXAMINER | |
|---|---|
| POPHAM, JEFFREY D | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

DATE MAILED: 01/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/925,031 | DI BERNARDO ET AL. | |
| | Examiner | Art Unit | |
| | Jeffrey D. Popham | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *30 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## *Remarks*

Claims 1-24 are pending.

## *Response to Arguments*

1. Applicant's arguments filed 9/30/2005 have been fully considered but they are not persuasive. Regarding the argument that there is no prompting, suggestion, or hint present in either of the references (Dachselt and Bianco) to combine them, so as to first confuse a message through a scrambler and then diffuse the confused document through a chaotic system; Page IV-519, section 4.2 of Dachselt teaches the cascading of ciphers. When viewing the combination of Dachselt-Bianco, one of ordinary skill in the art would use the cascading technique described in section 4.2 of Dachselt in order to cascade the encryption method of Bianco onto an encryption method of Dachselt. When used in this combination, the input to the encryption method in Bianco would be the output of the encryption method in Dachselt, which is a confused/scrambled string.

Regarding the argument that the coating metal layer in claim 20 is referring to a mechanism by which to increase the safety of the system and hiding the most sensitive elements on the chip; nowhere does this claim recite the use of the metal layer coating for such purposes. However, the reference Answers shows a coating metal layer, in the form of a heat sink, that covers a chip, thus hiding the elements of the chip.

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-19 and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dachselt (Dachselt et al., "Chaotic Versus Classical Stream Ciphers – A Comparative Study", *in Proceedings of the IEEE International Symposium on Circuits and Systems*, Monterey, CA, May 31 – June 3, 1998, pp. 518-521) in view of Bianco (U.S. Patent 5,048,086).

Regarding Claim 1,

Dachselt discloses a method comprising confusing characters belonging to an electronic input document through an invertible scrambler to obtain a confused document (Page IV-519, Section 3.4; and Page IV-520, Figure 2) and using two encryption algorithms in cascade (Page IV-519, Section 4.2), but does not disclose diffusing the confused document by mixing it with chaotic characters to obtain an encrypted document.

Bianco, however, discloses diffusing the document (which is the confused document in the combination) by mixing it with chaotic characters to obtain an encrypted document (Column 4, line 59 to Column 5, line 24). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the

chaotic encryption system of Bianco into the encryption system of Dachselt in order to increase robustness of the data against recovery by cryptanalysis, thus making the system more secure (Column 4, lines 8-48).

Regarding Claim 2,

Dachselt as modified by Bianco discloses the method of claim 1, in addition, Dachselt discloses that the confusing step comprises carrying out operations defined within a Galois field (Page IV-519, Section 3.1).

Regarding Claim 3,

Dachselt as modified by Bianco discloses the method of claim 1, in addition, Dachselt discloses that the electronic input document comprises a plurality of strings of characters to be encrypted, and the confused document comprises a plurality of confused characters, and the confusing step comprises adding each string of characters to be encrypted to strings of confusing characters obtained by multiplying the strings of confused characters by respective multiplication constants (Page IV-519, Section 3.4; and Page IV-520, Figure 2).

Regarding Claim 4,

Dachselt as modified by Bianco discloses the method of claim 3, in addition, Dachselt discloses that before being multiplied

by the multiplication constants, the strings of confused characters are delayed (Page IV-519, Section 3.4).

Regarding Claim 5,

Dachselt as modified by Bianco discloses the method of claim 1, in addition, Dachselt discloses that the confused document comprises a plurality of strings of confused characters (Page IV-519, Section 3.4; and Page IV-520, Figure 2); and Bianco discloses that the diffusing step comprises generating chaotic characters through a chaos generator and mixing the strings of confused characters with the chaotic characters (Column 4, line 59 to Column 5, line 24).

Regarding Claim 6,

Dachselt as modified by Bianco discloses the method of claim 5, in addition, Bianco discloses that the mixing step comprises performing an exclusive OR operation (Column 4, line 59 to Column 5, line 24).

Regarding Claim 7,

Dachselt as modified by Bianco discloses the method of claim 5, in addition, Bianco discloses that the chaos generator implements the function:

$f_k(x) = Kx(1 - x)$. (Column 3, lines 24-43).

Regarding Claim 8,

Dachselt as modified by Bianco discloses the method of claim 1, in addition, Dachselt discloses:

a) loading encryption keys into shift registers of the invertible scrambler (Page IV-519, Sections 3.3 and 3.4; and Page IV-520, Figure 2);

b) acquiring an input character string (Page IV-519, Section 3.4; and Page IV-520, Figure 2);

c) calculating a diffused character string using the input character string, the encryption keys, and the contents of the shift registers (Page IV-519, Section 3.4);

d) feeding the diffused character string to the shift registers, and issuing a command for a shift operation for the shift registers (Page IV-519, Section 3.4; and Page IV-520, Figure 2);

e) repeating b), c) and d) a preset number of times to obtain a plurality of the confused character strings (Page IV-519, Section 3.4; and Page IV-520, Figure 2);

Bianco discloses loading an initial chaotic value into a chaotic value register (Column 4, line 63 to Column 5, line 5);

f) calculating a subsequent chaotic value, using the contents of the chaotic value register (Column 5, lines 5-11);

g) adding the plurality of confused character strings to the subsequent chaotic value to obtain an encrypted word (Column 5, lines 12-24);

h) storing the subsequent chaotic value in the chaotic value register (Column 5, lines 12-24); and

i) repeating the encryption process on subsequent blocks of data (Column 5, lines 12-24).

Regarding Claim 21,

Claim 21 is a method claim that is broader than narrower method claim 8 and is rejected for the same reasons.

Regarding Claim 23,

Claim 23 is a method claim that is broader than narrower method claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Dachselt as modified by Bianco discloses the method of claim 8, in addition, Dachselt discloses that c) uses the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t - j)$$

In which IN(t) is the input character string, $c_j$ are the encryption keys, $s(t - j)$ are the contents of the shift registers, and s(t) is the diffused character string (Page IV-519, Section 3.4; and Page IV-520, Figure 2).

Regarding Claim 10,

Dachselt as modified by Bianco discloses the method of claim 8, in addition, Bianco discloses that f) uses the following relation:

$f_k(x) = Kx(1 - x)$;

where K is a bifurcation parameter of a chaotic system (Column 3, lines 24-43).

Regarding Claim 11,

Dachselt as modified by Bianco discloses the method of claim 1, in addition, Dachselt discloses unscrambling an encrypted document through an unscrambler opposite to the scrambler (Page IV-519, Section 3.4; and Page IV-520, Figure 2); and Bianco discloses decrypting an encrypted document by mixing it with the chaotic characters (Column 5, lines 25-41).

Regarding Claim 12,

Dachselt as modified by Bianco discloses the method of claim 3, in addition, Dachselt discloses that an encrypted document comprises a plurality of encrypted character strings (Page IV-519, Section 3.4; and Page IV-520, Figure 2),

The method comprising decrypting the encrypted document through a first and a second decryption operation, in cascade (Page IV-519, Section 4.2; and Page IV-520, Figure 2),

The second decryption operation supplying a plurality of decrypted characters strings (Page IV-519, Section 3.4; and Page IV-520, Figure 2),

The second decryption operation comprising an unscrambling step by subtracting each predecrypted character

string from feedback character strings obtained by multiplying the decrypted character strings by the multiplication constants (Page IV-519, Section 3.4; and Page IV-520, Figure 2).

Bianco discloses the first decryption operation comprising a mixing step wherein the encrypted character strings are mixed with the chaotic characters to obtain a plurality of predecrypted character strings (Column 5, lines 25-41).

Regarding Claim 13,

Dachselt discloses a device comprising:

A confusion block for confusing an electronic input document, the confusion block comprising an invertible scrambler that supplies a confused document (Page IV-519, Section 3.4; and Page IV-520, Figure 2); and that another encryption block is cascade-connected to the confusion block (Page IV-519, Section 4.2; and Page IV-520, Figure 2), but does not disclose that this second encryption block is a diffusion block comprising mixing means for mixing the confused document with chaotic characters, which supply an encrypted document.

Bianco, however, discloses a diffusion block comprising mixing means for mixing the confused document with chaotic characters, which supply an encrypted document (Column 4, line 59 to Column 5, line 24). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

incorporate the chaotic encryption system of Bianco into the encryption system of Dachselt in order to increase robustness of the data against recovery by cryptanalysis, thus making the system more secure (Column 4, lines 8-48).

Regarding Claim 14,

Dachselt as modified by Bianco discloses the device of claim 13, in addition, Dachselt discloses that the scrambler comprises operators acting within a Galois field (Page IV-519, Section 3.1).

Regarding Claim 15,

Dachselt as modified by Bianco discloses the device of claim 13, in addition, Dachselt discloses that the scrambler comprises an adding element having a first and a second input, the first input receiving a string of characters to be encrypted that belong to the electronic input document; a plurality of shift registers cascade-connected to one another and to the adding element; a plurality of multiplier elements, each having an input connected to an output of a respective shift register and to an own output; a plurality of adding nodes cascade-connected, each adding node having an input connected to the output of a respective multiplier element, an adding node arranged upstream and having a second input connected to a last multiplier element of the multiplier elements, and an adding node arranged downstream and having an output

connected to the second input of the adding element (Page IV-520, Figure 2).

Regarding Claim 16,

Dachselt as modified by Bianco discloses the device of claim 13, in addition, Bianco discloses that the mixing means comprise an EXOR logic circuit, and the diffusion block comprises a chaos generator (Column 4, line 59 to Column 5, line 24).

Regarding Claim 17,

Dachselt as modified by Bianco discloses the device of claim 16, in addition, Bianco discloses that the chaos generator implements the following function:

$f_k(x) = Kx(1 - x)$;

where K is a bifurcation parameter of a chaotic system (Column 3, lines 24-43).

Regarding Claim 18,

Dachselt as modified by Bianco discloses the device of claim 13, in addition, Bianco discloses integrating all of the components of the encryptor in one first chip (Column 6, lines 18-53).

Regarding Claim 19,

Dachselt as modified by Bianco discloses the device of claim 13, in addition, Bianco discloses integrating all of the components of the decryptor in a second chip (Column 6, lines 18-53).

Regarding Claim 22,

Dachselt discloses a method comprising:

Acquiring encryption keys (Page IV-519, Sections 3.3 and 3.4; and Page IV-520, Figure 2);

Acquiring input character strings (Page IV-519, Section 3.4; and Page IV-520, Figure 2);

Calculating diffused character strings using the input characters strings, the encryption keys and previous diffused character strings (Page IV-519, Section 3.4); and

Decrypting the encrypted words by subtracting them from previously decrypted words using an unscrambler element having a structure similar to that of the scrambler and using identical encryption keys (Page IV-519, Section 3.4; and Page IV-520, Figure 2);

But does not disclose acquiring an initial chaotic value, adding sets of diffused character strings to subsequent chaotic values generated by a chaotic processor to obtain encrypted words, or decrypting the encrypted words by adding the encrypted words to chaotic values identical to the encryption values.

Bianco, however, discloses acquiring an initial chaotic value (Column 4, line 63 to Column 5, line 5);

Adding sets of diffused character strings to subsequent chaotic values generated by a chaotic processor to obtain encrypted words (Column 5, lines 5-24); and

Decrypting the encrypted words by adding the encrypted words to chaotic values identical to the encryption values (Column 5, lines 25-41).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the chaotic encryption system of Bianco into the encryption system of Dachselt in order to increase robustness of the data against recovery by cryptanalysis, thus making the system more secure (Column 4, lines 8-48).

Regarding Claim 24,

Dachselt discloses a device for protecting the contents of an electronic document, comprising:

A confusion block for receiving and confusing an electronic input document (Page IV-519, Section 3.4; and Page IV-520, Figure 2), the confusion block comprising:

An invertible scrambler that supplies a confused document (Page IV-519, Section 3.4; and Page IV-520, Figure 2), the scrambler comprising operators acting within a Galois field (Page IV-519, Section 3.1),

The scrambler comprising an adding element having a first and a second input, the first input receiving a string of characters to be encrypted that belong to the electronic input document, a plurality of shift registers cascade-connected to one another and to

the adding element, a plurality of multiplier elements, each having an input connected to an output of a shift register and to its own output, a plurality of adding nodes cascade-connected, each adding node having an input connected to the output of a respective multiplier element, an adding node arranged upstream and having a second input connected to a last multiplier element of the multiplier elements, and an adding node arranged downstream and having an output connected to the second input of the adding element (Page IV-520, Figure 2); and

A second decryption block cascade-connected to the confusion block (Page IV-519, Section 4.2; and Page IV-520, Figure 2);

But does not disclose that the second decryption block is a diffusion block comprising a mixing circuit for mixing the confused document with chaotic characters to supply an encrypted document, the mixing circuit comprising an EXOR logic circuit, or that the diffusion block comprising a chaos generator that implements the function $f_k(x) = Kx(1 - x)$; where K is a bifurcation parameter of a chaotic system.

Bianco, however, discloses a diffusion block comprising a mixing circuit for mixing the confused document with chaotic characters to supply an encrypted document (Column 4, line 59 to Column 5, line 24), the mixing circuit comprising an EXOR logic

circuit (Column 4, line 59 to Column 5, line 24), and the diffusion block comprising a chaos generator that implements the following function:

$f_k(x) = Kx(1 - x)$;

where K is a bifurcation parameter of a chaotic system (Column 3, lines 24-43).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the chaotic encryption system of Bianco into the encryption system of Dachselt in order to increase robustness of the data against recovery by cryptanalysis, thus making the system more secure (Column 4, lines 8-48).

3. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dachselt in view of Bianco, further in view of Answers (Computer Desktop Encyclopedia, definition of "heat sink", 1998, pp. 1-2, obtained from http://www.answers.com/topic/heat-sink?method=5).

Dachselt as modified by Bianco does not disclose the use of a metal casing over the chip.

Answers, however, discloses that there is a metal casing [heat sink] over the chip (Pages 1-2, "Computer Desktop Encyclopedia" section). It would have been obvious to incorporate the heat sink of Answers into the

encryption system of Dachselt as modified by Bianco in order to absorb heat from the chip to cool it down.

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER